Network Management & Monitoring

NetFlow Overview
Netflow
- What it is and how it works
- Uses and Applications

Flow-tools
- Architectural issues
- Software, tools etc

Lab
Network Flows

• Packets or frames that have a common attribute.
• Creation and expiration policy – what conditions start and stop a flow.
• Counters – packets, bytes, time.
• Routing information – AS, network mask, interfaces.
Cisco’s Definition of a Flow

Unidirectional sequence of packets sharing

1. Source IP address
2. Destination IP address
3. Source port for UDP or TCP, 0 for other protocols
4. Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols
5. IP protocol
6. Ingress interface (SNMP ifIndex)
7. IP Type of Service
Network Flows

- Unidirectional or bidirectional.
- Bidirectional flows can contain other information such as round trip time, TCP behavior.
- Application flows look past the headers to classify packets by their contents.
- Aggregated flows – flows of flows.
Working with Flows

- Generate the flows from device (usually a router)
- Export flows from the device to collector
  - Configure version of flows
  - Sampling rates
- Collect the flows
  - Tools to Collect Flows - Flow-tools
- Analyze them
  - More tools available, can write your own
A Key with more elements will generate more flows.

Greater number of flows equals:
- More post processing time to generate reports
- More memory and CPU requirements for device generating flows
- More storage needed on the flow processing server

Depends on application. Traffic engineering vs. intrusion detection.
Flow Accounting

- Accounting information accumulated with flows.
- Packets, Bytes, Start Time, End Time.
- Network routing information – masks and autonomous system number.
Flow Generation/Collection

Passive monitor
- A passive monitor (usually a Unix host) receives all data and generates flows.
- Resource intensive

Router or other existing network device
- Router or other existing devices like switch, generate flows.
- Sampling is possible
- Nothing new needed
Passive Monitor Collection

Flow probe connected to switch port in "traffic mirror" mode
Passive Collector

- Using passive collection, not all flows in the network will be seen as opposed to collection from the router
- The collector will only see flows from the network point it is connected on
- However this method does relieve the router from processing netflows and exporting them
- Useful on links with only one entry into the network or where only flows from one section of the network are needed
Router Collection

Flow collector stores exported flows from router.
Router Collection

• With this method, all flows in the network can be observed
• However, more work for the router in processing and exporting the flows
• Optionally, one can choose on which interfaces netflow collection is needed and not activate it on others
• Also, if there is a router on each LAN, netflow can be activated on those routers to reduce the load on the core router
Cisco NetFlow

- Unidirectional flows.
- IPv4 unicast and multicast.
- Aggregated and unaggregated.
- Flows exported via UDP.
- Supported on IOS and CatOS platforms.
- Catalyst NetFlow is different implementation.
Cisco NetFlow Versions

- 4 Unaggregated types (1,5,6,7).
- 14 Aggregated types (8.x, 9).
- Each version has its own packet format.
- Version 1 does not have sequence numbers – no way to detect lost flows.
- The “version” defines what type of data is in the flow.
- Some versions specific to Catalyst platform.
NetFlow Version 1

- Accounting: Packets, Octets, Start/End time, Output interface
- Other: Bitwise OR of TCP flags.
- Obsolete
NetFlow Versions 2-4

- Cisco internal
- Were never released
NetFlow v5

- Accounting: Packets, Octets, Start/End time, Output interface.
- Other: Bitwise OR of TCP flags, Source/Destination AS and IP Mask.
- Packet format adds sequence numbers for detecting lost exports.
- IPv4 only
NetFlow v8

- Aggregated v5 flows.
- Not all flow types available on all equipments.
- Much less data to post process, but loses fine granularity of v5 – no IP addresses.
NetFlow v9

- IPv6 support
- Additional fields like MPLS labels
- Builds on earlier versions
• Configured on each input interface.
• Define the version.
• Define the IP address of the collector (where to send the flows).
• Optionally enable aggregation tables.
• Optionally configure flow timeout and main (v5) flow table size.
• Optionally configure sample rate.
Cisco IOS Configuration

ip flow-top-talkers
    top 10
    sort-by bytes

gw-169-223-2-0#sh ip flow top-talkers

<table>
<thead>
<tr>
<th>SrcIf</th>
<th>SrcIPaddress</th>
<th>DstIf</th>
<th>DstIPaddress</th>
<th>Pr</th>
<th>SrcP</th>
<th>DstP</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/1</td>
<td>169.223.2.2</td>
<td>Fa0/0</td>
<td>169.223.11.33</td>
<td>06</td>
<td>0050</td>
<td>0B64</td>
<td>3444K</td>
</tr>
<tr>
<td>Fa0/1</td>
<td>169.223.2.2</td>
<td>Fa0/0</td>
<td>169.223.11.33</td>
<td>06</td>
<td>0050</td>
<td>0B12</td>
<td>3181K</td>
</tr>
<tr>
<td>Fa0/0</td>
<td>169.223.11.33</td>
<td>Fa0/1</td>
<td>169.223.2.2</td>
<td>06</td>
<td>0B12</td>
<td>0050</td>
<td>56K</td>
</tr>
<tr>
<td>Fa0/0</td>
<td>169.223.11.33</td>
<td>Fa0/1</td>
<td>169.223.2.2</td>
<td>06</td>
<td>0B64</td>
<td>0050</td>
<td>55K</td>
</tr>
<tr>
<td>Fa0/1</td>
<td>169.223.2.2</td>
<td>Local</td>
<td>169.223.2.1</td>
<td>01</td>
<td>0000</td>
<td>0303</td>
<td>18K</td>
</tr>
<tr>
<td>Fa0/1</td>
<td>169.223.2.130</td>
<td>Fa0/0</td>
<td>64.18.197.134</td>
<td>06</td>
<td>9C45</td>
<td>0050</td>
<td>15K</td>
</tr>
<tr>
<td>Fa0/1</td>
<td>169.223.2.130</td>
<td>Fa0/0</td>
<td>64.18.197.134</td>
<td>06</td>
<td>9C44</td>
<td>0050</td>
<td>12K</td>
</tr>
<tr>
<td>Fa0/0</td>
<td>213.144.138.195</td>
<td>Fa0/1</td>
<td>169.223.2.130</td>
<td>06</td>
<td>01BB</td>
<td>DC31</td>
<td>7167</td>
</tr>
<tr>
<td>Fa0/0</td>
<td>169.223.15.102</td>
<td>Fa0/1</td>
<td>169.223.2.2</td>
<td>06</td>
<td>C917</td>
<td>0016</td>
<td>2736</td>
</tr>
<tr>
<td>Fa0/1</td>
<td>169.223.2.2</td>
<td>Local</td>
<td>169.223.2.1</td>
<td>06</td>
<td>DB27</td>
<td>0016</td>
<td>2304</td>
</tr>
</tbody>
</table>

10 of 10 top talkers shown. 49 flows processed.
Cisco Command Summary

• Enable CEF (done by default)
  - `ip cef`
• Enable flow on each interface
  ip route cache flow
  OR
  ip flow ingress
  ip flow egress

• View flows
  - `show ip cache flow`
  - `show ip flow top-talkers`
Cisco Command Summary

- Exporting Flows to a collector

  `ip flow-export version 5 [origin-as|peer-as]`
  `ip flow-export destination x.x.x.x <udp-port>`

- Origin AS will include the origin AS Number in the flow while Peer AS will only include the AS Number of the peering neighbor

- Exporting aggregated flows

  `ip flow-aggregation cache as|prefix|dest|source|proto enabled`
  `export destination x.x.x.x <udp-port>`
Flows and Applications
Uses for NetFlow

- Problem identification / solving
  - Traffic classification
  - DoS Traceback (some slides by Danny McPherson)

- Traffic Analysis and Engineering
  - Inter-AS traffic analysis
  - Reporting on application proxies

- Accounting (or billing)
  - Cross verification from other sources
  - Can cross-check with SNMP data
Detect Anomalous Events: SQL

“Slammer” Worm*

<table>
<thead>
<tr>
<th>Anomaly 125772 Detailed Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
</tr>
<tr>
<td>125772</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Affected Network Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router: nott 1.2.3.4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bitrate</th>
<th>Trailing</th>
<th>Expected</th>
<th>Difference</th>
<th>Missing</th>
</tr>
</thead>
<tbody>
<tr>
<td>27.89 Mbps</td>
<td>27.89 Mbps</td>
<td>27.89 Mbps</td>
<td>27.89 Mbps</td>
<td>27.89 Mbps</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Addresses</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source Addresses</th>
<th>Destination Addresses</th>
<th>Source Ports</th>
<th>Destination Ports</th>
<th>Source Interfaces</th>
<th>Destination Interfaces</th>
<th>Other Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.20.217/32</td>
<td>192.168.18.107/32</td>
<td>100.54 GB</td>
<td>415.466 GB</td>
<td>415.466 GB</td>
<td>415.466 GB</td>
<td>415.466 GB</td>
</tr>
</tbody>
</table>

Route Instability over Time

Traffic per UDP Port over Time
Once baselines are built anomalous activity can be detected

- Pure **rate-based** (pps or bps) anomalies may be legitimate or malicious
- Many **misuse** attacks can be immediately recognized, even **without** baselines (e.g., TCP SYN or RST floods)
- **Signatures** can also be defined to identify “interesting” transactional data (e.g., proto udp and port 1434 and 404 octets(376 payload) == slammer!)
- Temporal compound signatures can be defined to detect with higher precision
### Flow-based Commercial Tools...

#### Anomaly 150228

<table>
<thead>
<tr>
<th>ID</th>
<th>Importance</th>
<th>Duration</th>
<th>Start Time</th>
<th>Direction</th>
<th>Type</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>150228</td>
<td>High</td>
<td>17 mins</td>
<td>03:34, Aug 16</td>
<td>Incoming</td>
<td>Bandwidth (Profiled)</td>
<td>Microsoft 207.46.0.0/16windowsupdate.com</td>
</tr>
</tbody>
</table>

#### Traffic Characterization

<table>
<thead>
<tr>
<th>Sources</th>
<th>204.38.130.0/24</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>204.38.130.192/26</td>
</tr>
<tr>
<td></td>
<td>1024 - 1791</td>
</tr>
<tr>
<td>Destination</td>
<td>207.46.248.234/32</td>
</tr>
<tr>
<td></td>
<td>80 (http)</td>
</tr>
<tr>
<td>Protocols</td>
<td>tcp (6)</td>
</tr>
<tr>
<td>TCP Flags</td>
<td>S (0x02)</td>
</tr>
</tbody>
</table>

#### Affected Network Elements

<table>
<thead>
<tr>
<th>Router</th>
<th>Importance</th>
<th>Expected</th>
<th>Observed bps</th>
<th>Observed pps</th>
</tr>
</thead>
<tbody>
<tr>
<td>n1-chi3</td>
<td>High</td>
<td>pps</td>
<td>Max</td>
<td>Mean</td>
</tr>
<tr>
<td>Interface 67 at-1/1/0.14</td>
<td>198.110.131.125</td>
<td>26</td>
<td>832 K</td>
<td>563.1 K</td>
</tr>
<tr>
<td>pvc to WMU</td>
<td>2.6 K</td>
<td>1.7 K</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Anomaly Comments
Commercial Detection: A Large Scale DOS Attack
Accounting

Flow based accounting can be a good supplement to SNMP based accounting.
References

- flow-tools:
  http://www.splintered.net/sw/flow-tools
- WikiPedia:
  http://en.wikipedia.org/wiki/Netflow
- NetFlow Applications
  http://www.inmon.com/technology/netflowapps.php
- Netflow HOW-TO
  http://www.linuxgeek.org/netflow-howto.php
- IETF standards effort:
References

- Abilene NetFlow page
  http://abilene-netflow.itec.oar.net/

- Flow-tools mailing list:
  flow-tools@splintered.net

- Cisco Centric Open Source Community
  http://cosi-nms.sourceforge.net/related.html

- Cisco NetFlow Collector User Guide